1. Record Nr. UNINA9910255004903321

Autore	Al-Shaer Ehab
Titolo	Security and Resiliency Analytics for Smart Grids : Static and Dynamic Approaches / / by Ehab Al-Shaer, Mohammad Ashiqur Rahman
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2016
ISBN	3-319-32871-9
Edizione	[1st ed. 2016.]
Descrizione fisica	1 online resource (XVI, 144 p. 37 illus., 22 illus. in color.)
Collana	Advances in Information Security, , 1568-2633 ; ; 67
Disciplina	621.31028558
Soggetti	Computer security Computer networks Application software Data encryption (Computer science) Systems and Data Security Computer Communication Networks Information Systems Applications (incl. Internet) Cryptology
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references at the end of each chapters and index.
Nota di contenuto	Smart Grids and Security Challenges -- Analytics for Smart Grid Security and Resiliency -- Security Analytics for AMI and SCADA -- Security Analytics for EMSE Modules -- Intrusion Detection Systems for AMI -- Resiliency Threat Analysis for SCADA. .
Sommario/riassunto	This book targets the key concern of protecting critical infrastructures such as smart grids. It explains various static and dynamic security analysis techniques that can automatically verify smart grid security and resiliency and identify potential attacks in a proactive manner. This book includes three main sections. The first presents the idea of formally verifying the compliance of smart grid configurations with the security and resiliency guidelines. It provides a formal framework that verifies the compliance of the advanced metering infrastructure (AMI) configurations with the security and resiliency requirements, and generates remediation plans for potential security violations. The

second section covers the formal verification of the security and resiliency of smart grid control systems by using a formal model to analyze attack evasions on state estimation, a core control module of the supervisory control system in smart grids. The model identifies attack vectors that can compromise state estimation. This section also covers risk mitigation techniques that synthesize proactive security plans that make such attacks infeasible. The last part of the book discusses the dynamic security analysis for smart grids. It shows that AMI behavior can be modeled using event logs collected at smart collectors, which in turn can be verified using the specification invariants generated from the configurations of the AMI devices. Although the focus of this book is smart grid security and resiliency, the included formal analytics are generic enough to be extended to other cyber-physical systems, especially those related to industrial control systems (ICS). Therefore, industry professionals and academic researchers will find this book an exceptional resource to learn theoretical and practical aspects of applying formal methods for the protection of critical infrastructures.